

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 September 2001 (20.09.2001)

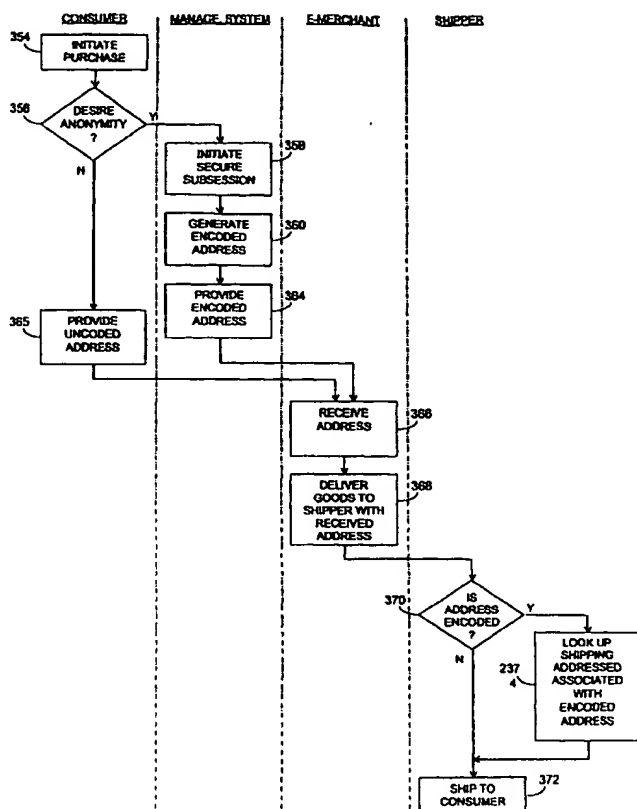
PCT

(10) International Publication Number
WO 01/69914 A2

- (51) International Patent Classification⁷: **H04N** (72) Inventors; and
(75) Inventors/Applicants (for US only): **ANDREWS, Dennis, W.** [US/US]; 6620 Epping Forest Way North, Jacksonville, CA 32217 (US). **HOSHIKO, Brian, L.** [US/US]; 1103 Quail Street, Newport Beach, CA 92660 (US).
- (21) International Application Number: **PCT/US01/08547**
- (22) International Filing Date: **14 March 2001 (14.03.2001)**
- (25) Filing Language: **English** (74) Agent: **SATERMO, Eric, K.**; P.O. Box 19099, Irvine, CA 92623-9099 (US).
- (26) Publication Language: **English**
- (30) Priority Data:
60/189,287 14 March 2000 (14.03.2000) US
09/644,109 21 August 2000 (21.08.2000) US
09/753,129 30 December 2000 (30.12.2000) US
09/753,274 30 December 2000 (30.12.2000) US
09/772,169 29 January 2001 (29.01.2001) US
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (71) Applicant (for all designated States except US): **ECAT-ALYSTONE.COM, INC.** [US/US]; 1103 Quail Street, Newport Beach, CA 92660 (US).
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: **METHODS FOR MANAGING TRANSACTIONS ON THE INTERNET WITH ANONYMOUS SHIPPING ADDRESSES**



(57) Abstract: A method of managing a transaction on the Internet between a consumer and an e-merchant in which the actual shipping address of the consumer is not provided to the merchant. When a consumer initiates a purchase with an e-merchant, if anonymity is desired, the consumer causes a management system to generate an encoded address. The encoded address may be a unique address code stored in a database in the management system and is associated with the actual shipping address of the consumer. The encoded address is provided to the e-merchant. The e-merchant may then prepare the goods for shipping and deliver the packaged goods to a shipper with the encoded address. The shipper then determines whether the address on the packaged goods is an encoded address or an actual shipping address. If the address is encoded, then the shipper may retrieve the actual shipping address associated with the encoded address from a database. Once the actual shipping address is obtained, the goods may be shipped to the consumer.

WO 01/69914 A2



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

**METHODS FOR MANAGING TRANSACTIONS ON THE INTERNET
WITH ANONYMOUS SHIPPING ADDRESSES**

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority on U.S. Provisional Application for Patent No. 60/189,287 filed March 14, 2000, and is a continuation-in-part (CIP) application of U.S. Patent Application Serial No. 09/772,169, filed January 29, 2001, which application is a CIP of U.S. Patent Application Serial Nos. 09/753,129 and 09/753,274 filed December 30, 2000, each of which is a CIP application of U.S. Patent Application Serial No. 09/644,109 filed August 21, 2000, the entire disclosure of each of which is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to the electronic commerce over a communication network such as the Internet and, more specifically, to systems for securely exchanging monetary value for goods and services purchased over the Internet. The present invention relates to systems and associated methodology for managing economic exchange between merchants and consumers anonymously and without a consumer providing an actual shipping address to a merchant.

BACKGROUND OF THE INVENTION

With the advent and looming dominance of the Internet in today's consumer market, conventional currency transactions between consumers and merchants have been redefined. Gone are the days of exclusive cash, check, or credit card transactions. Financial institutions and web merchants have had to develop new transaction techniques to ensure the integrity of the transaction and to maintain the privacy of the consumer.

Automation has achieved some of these qualities for large transactions through computerized electronic funds transfer (EFT) systems. Electronic funds transfer is essentially a process of value exchange achieved through a banking system's centralized computer transactions. EFT services are a transfer of payments utilizing electronic checks, which are used primarily by large commercial organizations.

Examples of EFT systems utilized by retail and commercial organizations include an automated clearing house (ACH) where a user can enter a pre-authorized code and download information with billing occurring later, and a point-of-sale (POS) system where a transaction is processed by connecting with a central computer for authorization for the transaction granted or

denied immediately. However, the payments made through these types of EFT systems are limited in that they cannot be performed without the banking system. Current EFT systems, credit cards, or debit cards, which are used in conjunction with an on-line system to transfer money between accounts, such as between the account of a merchant and that of a customer, cannot satisfy the need for an automated transaction system providing an ergonomic interface.

To implement an automated, convenient transaction that can dispense some form of economic value, there has been a trend towards off-line payments. For example, numerous ideas have been proposed for some form of electronic money that can be used in cashless payment transactions as alternatives to the traditional currency and check types of payment systems. See, for example, U.S. Patent No. 4,977,595, entitled "Method and Apparatus for Implementing Electronic Cash," and U.S. Patent No. 4,305,059, entitled "Modular Funds Transfer System." Other techniques for automated transactions include magnetic stripe cards purchased for a given amount and from which a prepaid value can be deducted for specific purposes. Other examples include memory cards or so called smart cards which are capable of repetitively storing information representing value that is likewise deducted for specific purposes.

In an electronic environment, it is desirable for a computer operated under the control of a merchant to obtain information offered by a customer and transmitted by a computer operating under the control of the customer over a publicly accessible packet-switched network (e.g., the Internet) to the computer operating under the control of the merchant, without risking the exposure of the information to interception by third parties that have access to the network, and to assure that the information is from an authentic source. It is further desirable for the payment processing to be flexible and able to negotiate with the client customer to select a mutually acceptable payment protocol and other payment options.

One such attempt to provide a secure transmission channel is a secure payment technology known as the Secure Electronic Transaction (SET), jointly developed by the Visa and MasterCard card associations. Other such secure payment technologies include Secure Transaction Technology (STT), Secure Electronic Payments Protocol (SEPP), Internet Keyed Payments (iKP), Net Trust, and Cybercash Credit Payment Protocol. Such secure payment technologies require the customer to operate software that is compliant with the secure payment technology, interacting with third-party certification authorities, thereby allowing the customer to transmit encoded information to a merchant, some of which may be decoded by the merchant, and some which can be decoded only by a payment gateway specified by the customer.

Another attempt to provide a secure transmission channel is a general-purpose secure communication protocol known as Secure Sockets Layer (SSL) developed by Netscape, Inc. SSL provides a means for secure transmission between two computers. SSL has the advantage that it does not require special-purpose software to be installed on the customer's computer because it is already incorporated into widely available software that many people utilize as their standard Internet access medium, and does not require that the customer interact with any third-party certification authority. Instead, the support for SSL may be incorporated into software already in use by the customer, e.g., the Netscape Navigator browser. However, although a computer on an SSL connection may initiate a second SSL connection to another computer, a drawback to the SSL approach is each SSL connection supports only a two-computer connection. Therefore, SSL does not provide a mechanism for transmitting encoded information to a merchant for retransmission to a payment gateway such that a subset of the information is readable to the payment gateway but not to the merchant. Although SSL allows for robustly secure two-party data transmission, it does not meet the ultimate need of the electronic commerce market for robustly secure three-party data transmission. Other examples of general-purpose secure communication protocols include Private Communications Technology (PCT) from Microsoft, Inc., Secure HyperText Transport Protocol (SHTTP) from Theresa Systems.

Internet-based payment solutions require security measures that are not found in conventional point-of-sale (POS) terminals. This additional requirement is necessitated because Internet communication is done over publicly accessible, unsecured communication lines, which is in stark contrast to the private, secure, dedicated phone or leased line service utilized between a traditional merchant and an acquiring bank. Thus, it is critical that any solution utilizing the Internet for a communication backbone employ some form of cryptography.

Prepaid instruments in use today are a variant of one of (or combination of several of) the following devices: prepaid phone and access cards, debit cards, and money orders and gift certificates. Most Debit Cards are predicated on a credit system or linked to an existing bank account. Internet purchase schemes are predominantly credit systems. In addition, a number of on-line purchase schemes utilize an electronic wallet that is filled (i.e., funded) and refilled from a credit source. This is synonymous to certain toll-road systems that debit a credit account periodically to pay in advance for toll road use that is often electronically sensed. Internet purchasing schemes to date are all credit or bank account based due to the inability to collect cash over the wire.

In view of the foregoing, there remains a need in the art for systems for managing financial transactions over the Internet in an efficient and versatile manner.

BRIEF SUMMARY OF THE INVENTION

The present invention provides methods for managing transactions over the Internet in which a consumer does not need to provide an actual shipping address to a merchant. Accordingly, the consumer maintains a level of anonymity not possible by using, for example, a post office box.

According to one aspect of the present invention, when a consumer initiates a purchase with an e-merchant, if anonymity is desired, the consumer may cause a management system to generate an encoded address. The encoded address may be a unique address code stored in a database in the management system and is associated with the actual shipping address of the consumer. The encoded address may be based on consumer input and/or encrypted information. Preferably, the encoded address includes the ZIP code of the actual shipping address of the consumer so that the merchant may calculate actual shipping charges.

Once generated, the encoded address is provided to the e-merchant. Accordingly, the e-merchant does not receive or know the consumer's actual shipping address. The e-merchant may then prepare the goods for shipping and deliver the packaged goods to a shipper with the encoded address. The shipper may be, for example, the U.S. Postal Service, United Parcel Service, FedEx, and so on.

The shipper then determines whether the address on the packaged goods is an encoded address or an actual shipping address. If the address is encoded, then the shipper may look up the actual shipping address associated with the encoded address. This may be accomplished by the shipper querying the management system which, in turn, may retrieve the actual shipping address in a database and then transmit the same to the shipper. Alternatively, the management system may provide the shipper with the encoded address and the actual shipping address after the encoded address is first generated. The shipper may store the encoded address and associated actual shipping address in a database and maintain the database of a plurality of encoded addresses and associated actual shipping addresses for future use. In either case, once the actual shipping address is obtained, the goods may be shipped.

Other aspects, features, and advantages of the present invention will become apparent to those skilled in the art from a consideration of the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. 1 is a block diagram of an exemplary e-commerce system according to the present invention in which prepaid monetary instruments are utilized by a system for managing transactions between consumers and e-merchants;

5 FIG. 2 is a schematic representation of a prepaid monetary instrument configured according to a preferred embodiment of the invention;

FIG. 3 is a flow chart illustrating exemplary methodology for managing anonymous transactions over a network with prepaid monetary instruments in accordance with the present invention;

10 FIG. 4 is a block diagram of an management system configured in accordance with an exemplary embodiment of the present invention;

FIGS. 5A and 5B are a schematic representations of Internet activation browser windows exemplifying principles of the present invention;

15 FIG. 6 is a schematic representation of an e-merchant verification browser window exemplifying principles of the present invention;

FIG. 7 is a block diagram of an exemplary e-commerce system according to the present invention in which transactions between consumers and merchants are carried out by proxy;

FIG. 8 is a flow chart illustrating exemplary methodology for managing transactions over the Internet by proxy in accordance with the present invention;

20 FIG. 9 is a schematic representation of a proxy payment browser window exemplifying principles of the present invention;

FIG. 10 is a flow chart illustrating exemplary methodology for managing check and money order transactions over the Internet in accordance with the present invention;

25 FIG. 11 is a flow chart illustrating exemplary methodology for managing transactions over the Internet by single-use credit-card numbers, or surrogate numbers, in accordance with a preferred embodiment of the present invention, particularly managing such transactions by proxy;

FIG. 12 is a flow chart illustrating exemplary methodology for managing transactions with surrogate numbers in accordance with an alternative embodiment of the invention;

30 FIG. 13 is a flow chart illustrating exemplary methodology for managing transactions without a consumer providing an actual shipping address to an e-merchant; and

FIG. 14 is a block diagram illustrating exemplary encoded address of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides in general apparatus and associated methodology for managing transactions between consumers and merchants over the Internet. These apparatus and methods include plural preferred embodiments, a number of which are described below. Those skilled in the art will appreciate that the following description provides foundation for many other embodiments that fall within the broad principles of the present invention as set forth in the appended claims.

Anonymous Transactions

Referring more particularly to the drawings, an exemplary embodiment of an e-commerce system according to the present invention is shown in FIG. 1 and is indicated generally by reference numeral 50. Exemplary e-commerce system 50 includes a management system 52 that is configured to allow anonymous transactions to take place between consumers 54 and merchants 56 over a network 58 such as the Internet. More specifically, through the use of prepaid monetary instruments purchased at one or more distributors 60, exemplary management system 52 enable consumers 54 to purchase goods and services from the merchants 56 with complete anonymity. In addition, exemplary management system 52 guarantees that the merchants 56 receive funds for goods and services provided without the drawbacks of conventional financial-transaction instruments such as credit cards. In a preferred embodiment, the management system 52 of the present invention provides cash-like and real-time transactions for purchases made on the Internet.

An example of a prepaid monetary instrument configured in accordance with the present invention is illustrated in FIG. 2 and is indicated by reference numeral 62. Exemplary instrument 62 includes information specific thereto, for example, a denomination or monetary value 64 and a security code 66 such as a serial number. In a preferred embodiment, exemplary instrument 62 may include one or more enablement means, such as a barcode 72 and/or a magnetic strip 74, which will be discussed in more detail below. Preferably, the instrument 62 of the present invention also includes an area 76 for graphics and text. Although any tangible form may be used, exemplary instrument 62 is preferably configured on a card-like body 78 for easy transport and familiarity. Exemplary instrument 62 may be preprinted or, alternatively, may have the monetary value 64 and the security code 66 printed at the time and place of the sale.

With further reference to FIG. 1, to place the principles of the invention in context, exemplary e-commerce system 50 generally includes a plurality of consumers 54a, 54b, 54c, ...,

54*k* each with access to a computer 80*a*, 80*b*, 80*c*, ..., 80*l* connected to the network 58. Each consumer 54 has direct access to a plurality of distributors 60*a*, 60*b*, 60*c*, ..., 60*m* of the instruments 62 and network access via a respective computer 80 to the management system 52 and a plurality of participating web merchants 56*a*, 56*b*, 56*c*, ..., 56*n*. The network 58 may
5 include the Internet 81 and an instrument services network 82, which is discussed in more detail below.

With additional reference to FIG. 3, each consumer 54 purchases an instrument 62 from any one of the distributors 60 (step 83). The plurality of distributors 60 may include retail establishments, convenience stores, department stores, post offices, dedicated kiosks, and so on.
10 In addition, the plurality of distributors 60 may include unattended devices, such as vending machines. The distributor 60 making the sale of the instrument 62 receives funds (step 84) from the consumer 54 in the amount of a desired monetary value 64. An additional service charge may be added in the sale of the instrument 62.

The distributor 60 then enables the instrument 62 (step 86), which may be accomplished
15 in any number of ways. For example, the barcode 72 may be optically scanned, or the magnetic strip 74 may be swiped through a reader such as a standard Verafone® interface. By enabling the instrument 62, the information specific thereto, i.e., the monetary value 64 and the security code 66, is transmitted via the network 58 to the management system 52 (step 88). The enablement of the instrument 62 preferably takes place across the instrument services network 82 of the system
20 network 58.

Referencing FIG. 4, the information transmitted by the distributor 60 is received by the management system 52 (step 90) at an instrument services gateway 92 which, in turn, sends the information to an enablement processor 94 which triggers an electronic transfer of funds (step 96). The distributor 60 electronically transfers funds (step 98) to the management system 52, and
25 an enabled account is established (step 100) for the instrument 62 via an enablement application program interface (API) 102. Enablement of an instrument 62 changes an account specific to the instrument from a pending status to an enabled status. Data associated with instruments 62 with accounts having an enabled status (i.e., enabled accounts) may be stored on an instruments data structure 104, and data associated with the transfer of funds from the distributors 60 may be
30 stored on a distributor data structure 106. In alternative embodiments, the distributor 60 may provide the monetary value 64 of the instrument 62, and the management system 52 may confirm the enablement of the instrument 62 with the distributor 60 and verify the monetary value 64.

A consumer 54 with an enabled instrument 62 then needs to activate the instrument 62 (step 108). To do so, the consumer 54 accesses an activation website (step 110) with a computer 80. The activation website may be part of a general customer website 112 maintained by the management system 52. Alternatively, the activation website may be a frame within a website of a distributor. Referencing FIG. 5A, a first activation window 114 is displayed on the consumer's computer 80 which prompts the consumer 54 for the security code 66 of the instrument 62 (step 116). The first activation window 114 may include fields for this information, as indicated by reference numeral 118. The consumer 54 may then activate a SUBMIT icon 120 to provide the security code 66 to the management system 52 (step 122).

Upon receipt of the security code 66, the management system 52 causes a second activation window 124 as shown in FIG. 5B to be displayed on the consumer's computer 80 which prompts the consumer 54 for a user ID and a password (step 125). The second activation window 124 may include fields for this information, as indicated by reference numerals 126 and 127, respectively. In a preferred embodiment, the second activation window 124 also includes fields for prompting the consumer for a challenge phrase and a challenge response, as indicated by reference numerals 128 and 129, respectively, which will be discussed in more detail below. Upon entering the requested information, the consumer 54 may then activate a SUBMIT icon 130 to provide the user ID and the password to the management system 52 (step 131).

The management system 52 receives the user ID and the password by an account activator 132, as shown in FIG. 4. Through an activation API 134, the enabled account associated with the instrument 62 is activated (step 136); that is, the enabled status of the account is changed to an active status. Data associated with the activated account of the instrument 62 may be stored on an active accounts data structure 138.

With the account associated with an instrument 62 activated, a consumer 54 is free to shop on-line at any merchant with a website connected to the network 58 and set up to accept payment with the instrument 62 of the present invention. To do so, the consumer 54 accesses a merchant website (step 140) to shop for goods and services. When the consumer 54 has decided upon a desired selection of goods and/or services, a purchase is initiated (step 142) from the merchant's website. When a purchase is initiated, the merchant 56 preferably redirects the consumer 54 to the management system 52 (step 143). A secure handshake between the customer 54 and the management system 52 may be established.

Referencing FIG. 6, when the purchase is initiated, a verification window 144 may be

displayed on the consumer's computer 80 which prompts the consumer 54 for the user ID and the password (step 146). The verification window 144 may include fields for this information, as indicated by reference numerals 148 and 149, respectively. In alternative embodiments, for example, if a secure handshake is not established, the verification window 144 may also include
5 a field for prompting the consumer for the challenge phrase and the challenge response, similar to that shown in FIG. 5B. This is particularly useful as added security if a prepaid instrument 62 is lost or stolen, or if the consumer is utilizing a computer 80 other than that used to activate the account associated with the prepaid instrument. The consumer 54 may then activate a SUBMIT icon 152 to provide the user ID and the password to the management system 52 (step 154).

10 Upon receiving the user ID and the password, the management system 52 generates and transmits a query to a transaction engine 160. Upon receipt of the query, the transaction engine 160 validates the user ID and the password and correlates this information with active account information in the active account data structure 138 through a prepaid transaction API 164. The funds in the account are then verified (step 166). A funds signal is generated and transmit (step
15 168) to the merchant 56. The funds signal contains information indicative of whether or not sufficient funds are in the account to cover the purchase.

Upon receipt of the funds signal (step 170), the merchant 56 proceeds with the transaction if sufficient funds are available (step 172). If sufficient funds are not available, the management system 52 may query the customer 54 for alternative or addition payment options, such as a
20 credit card to cover the deficit. The merchant 56 then transmits a verification (step 174) to the customer 54 that the transaction has taken place. Upon receipt of the verification (step 176), the customer 54 may continue shopping with the instrument 62 if funds remain in the account (step 178).

Upon completing the transaction, the merchant 56 may send a purchase signal (step 180)
25 to the management system 52 which, upon receipt (step 182), debits the account (step 184) of the instrument 62 associated with the transaction. The management system 52 may then transfer funds (step 186) to the merchant which, upon their receipt (step 188), completes the anonymous transaction between the customer 54 and the merchant 56. The amount of funds transferred to the merchant 56 is based upon the purchase price and may be reduced by a service charge of the
30 management system. Alternatively, the management system 52 may debit the account of the prepaid instrument 62 prior to transmitting the funds signal in step 168.

One of the advantages of the management system 52 of the present invention is that

purchases made by a customer may be batched or pre-authorized. According to this feature of the invention, a merchant 56 batches multiple purchases made during a single on-line session with a consumer 54. To do so, an advance is established by completing a secure handshake between the merchant 56 and the management system 52 and between the merchant 56 and the consumer 54. When the shopping session is complete, the total amount is communicated to the management system 52 and the consumer 54 to finalize the transaction. This embodiment is particularly useful for merchants who specialize as content or information providers. Such merchants require micropayments for various informational units. Micropayments are small payments that are not suitable for credit-based purchase schemes, examples of which include \$0.25 for a download of a piece of intellectual property and \$1.50 for two viewing/use rights for an on-line service such as financial information from a financial website.

In a preferred embodiment, exemplary management system 52 is configured to allow the combining of the accounts of multiple instruments into a single account. For example, if a single consumer 54 has purchased several instruments and has used these instruments such that a small balance remains in the account of each, then the consumer 54 may combine these multiple accounts into a single account that can be used analogously to a new account. In other words, Account 1 through Account x may be combined into Account $x+1$. Accounts 1 through x would then be empty and marked idle.

This account combination feature of the management system 52 may be carried out by a customer query handler 190 and an account services API 192. A data structure 194 dedicated to quiet and closed accounts may be provided to house data associated with the accounts comprising the combined account. In addition to combining accounts, customer query handler 190 may be configured to enable a consumer to move or transfer funds from one account to another.

Conversely to the combination of accounts, the management system 52 of the present invention may be configured to allow the parsing or splitting of one account into several accounts. Parsing provides an effective way to disperse of a remaining balance in an account, and may be carried out by the customer query handler 190.

The management system 52 of the present invention may also include a data structure 196 for housing data relevant to each of the merchants 56 of the network 50. In doing so, the management system 52 may organize the merchant 56 into categories according to, for example, the type of goods or services being sold, the target consumer (e.g., teens, adult only, etc.), and the

type of offerings (e.g., information, soft services, or hard goods). By classifying the merchants 56 in an object class library structure, the process of adding and grouping new merchants 56 is greatly simplified. This classification enables the creation of prepaid monetary instruments 62 that are valid only at certain specifiable classes of merchants 56.

5 For example, one of the most useful such class of merchants 56 would be suitable for preteens and teens. Accordingly, a "card for minors" may be enabled that is restricted to merchants 56 that have been so categorized. As new merchants 56 come on-line and meet the qualifications, they may be added to this category of merchants and available to the "cards for minors," as well as to all newly issued cards.

10 This categorization of merchants 56 is preferably monitored and maintained current. If an existing participating merchant changes its offerings goods and/or services in such a way that it would change its categorization, then such a change may be detected and updated for existing accounts, as well as new accounts. This monitoring and updating may be accomplished by the combination of the object class library classification and an automated "web crawling" of each
15 merchant 56. This form of electronic inspection may be performed periodically (e.g., daily) against all participating merchants 56. The activated instruments 62 may then be enabled or disabled according to the current classes of merchants 56.

With further reference to FIG. 4, exemplary management system 52 may also provide a website 198 for access by the merchant 56 of the system 50. A merchant query handler 200 and
20 a merchant SVC 202 in communication with the merchant data structure 196 may be configured to handle queries from merchants 56 as to status of there respective accounts with the system.

The accounts of the management system 52 may be classified according to status. For example, accounts may be allocated by the security codes or a block of security codes to a particular distributor 60. The allocation of accounts within the management system 52 allows a
25 distributor 60 to design and manufacture unique instruments 62. A pending account indicates an account that is on-line in the system 52 and awaiting enablement. An enabled account, as discussed above, indicates that the account has been purchased and enabled and is awaiting activation. An activated account, also as discussed above, indicates that the account has been activated by the consumer 54 on the customer website 112.

30 An account may acquire a quiet status if the account balance goes to zero (or effective zero) and/or has seen not activity for a predetermined amount of time, for example, three months. In addition, an account may acquire a complete status if the account has been quiet for an

extended predetermined amount of time, for example, at least 24 months with a balance or six months with no effective balance. The active accounts data structure 138 and the quiet/closed accounts data structure 194 may include data related to each of these accounts.

According to transaction-management methodology of the present invention, the enablement processor 94 processing a signal from a distributor 60 received via the network 58. The signal from the distributor 60 includes the information, i.e., the monetary value 64 and the security code 66, of the prepaid instrument 62. The enablement processor 94 then causes an account associated with the prepaid instrument to be enabled based upon the information. The account activator 132 then receives a signal from a customer 54 via the network 58. The signal from the customer 54 includes at least the security code, the user ID, and the password. The account activator 132 then causes the enabled account associated with the security code to be activated in association with the user ID and the password. The transaction engine 160 then processes a signal from including information regarding a purchase and a password. The transaction engine 160 causes a verification of funds in the active account associated with the received user ID and password and causes a signal to be generated and transmitted to the merchant 56 as to whether the account associated with the password has sufficient funds to cover the purchase. The transaction engine 160 then receives and processes a second signal from the merchant 56, with the second signal including information indicative of whether the purchase took place. The transaction engine 160 causes funds to be transferred to the merchant 56 based upon a value of the purchase.

The foregoing methodology may be implemented in software modules including a plurality of code segments. For example, the software may include code segments for processing the signal from the distributor and for enabling the account associated with the prepaid instrument 62 in the enablement processor 94. Other code segments may be configured to activate the account and associate the account with a user ID and a password received by the account activator 132. Additional code segments may be configured for processing the signal from the merchant 56 to the transaction engine 160, including code segments for prompting the consumer for the user ID and the password associated with the instrument, for verifying sufficient funds, for generating the signal, and for causing the signal to be transmitted to the merchant as to the same. The software may also include other code segments for processing the second signal from the merchant 56 and for causing funds to be transferred to the merchant based upon a value of the purchase.

Proxy Transactions

A preferred embodiment of an e-commerce system of the present invention is illustrated in FIG. 7 and indicated generally with reference numeral 250. Exemplary e-commerce system 250 includes a proxy management system 252 for managing transactions between a consumer 54 and a merchant 56 by proxy. Exemplary proxy system 252 includes a proxy server 254 and a portal web site 256. The proxy server 254 is configured to be accessible to the consumer 54 by a computer 80 with a web browser 257 and to one or more merchant servers 258 via the Internet 81. Each merchant server 258 is configured to host one or more merchant web sites 118. The portal web site 256 may be hosted by the proxy server 254 if desired or, alternatively, by another server, such as a portal server 259 or a server of a distributor as discussed above. For clarity, only a single consumer and merchant are shown in FIG. 7, although a plurality of each are contemplated analogous to that shown in FIG. 1.

According to the present invention, the consumer 54 is able to carry out transactions with the merchant 56 without needing to access the merchant server 258 directly. Such a proxy system has a number of advantages. For example, analogous to that described above, the consumer 54 may establish a prepaid account with the proxy management system 252 and then use funds in the prepaid account to carry out transactions with merchants 56. In addition, with prepaid accounts, the consumer 54 need not be concerned with the payment modes (i.e., credit card, check, money order, etc.) of each merchant 56, because the proxy server 254 acts as a middleman between the consumer 54 and the merchant 56. In other words, regardless of the modes of payment accepted by the merchant 56, the consumer 54 may use any type of desired mode of payment, and vice versa.

With additional reference to FIG. 8, to carry out a transaction by proxy, a consumer 54 first accesses the portal web site 256 with a computer 80 (step 260), which site is hosted by a server other than that of the merchant server 258, e.g., the portal server 259. The consumer 54 may then access any merchant web site 118 (step 264) via the portal web site 256, e.g., by clicking on a link on the browser 257. This causes the server hosting the portal web site 256 to communicate with the proxy server 254 to request the desired merchant web site. The proxy server 254 then connects with the merchant server 258 (step 266) hosting the desired merchant web site 118 (step 268), and retrieves the merchant web site 118 (step 270). The merchant web site 118 is now presented to the browser 257 of the consumer 54. This may be accomplished by the proxy server 254 first parsing the merchant web site 118 and then sending web pages of the

site 118 to the browser 257. The consumer 54 may now view the merchant web site 118 (step 271).

The proxy server 254 is configured so that the consumer 54 is able to view, navigate, and browse the merchant web site 118 (step 272) within the portal web site 256 via the proxy server 254 as though the consumer computer 80 were connected directly to the merchant server 258. In addition, the proxy server 254 is configured to modify and update the merchant web site 118 (step 274) in real time in response to browsing by the consumer 54 which, for the purposes of this description, is called "mapping." For example, as the consumer 54 activates links within a web page of the merchant web site 118, the proxy server 254 presents the new links as provided by merchant server 258 (step 275) by parsing the merchant web site 118 in real time. The web pages associated with the activated links are then mapped to the browser 257 on the consumer's computer 80.

When the consumer 54 initiates a transaction (step 276), the proxy server 254 captures payment information (step 277) provided by the merchant 56 (step 278), which information may include price, tax, shipping and handling costs, and so on. The proxy server 254 then provides a proxy payment page or window (step 280) to the browser 257, an example of which is shown in FIG. 9 and indicated by reference numeral 282. Exemplary proxy payment page 282 may include a number of payment fields, for example, a mode of payment field 284 and a shipping field 286, and a submit icon 288. To carry out the transaction, the consumer 54 completes the necessary payment fields and submits the information to the proxy server 254 (step 290).

The proxy server 254 then secures funds (step 292) in accordance with the mode of payment 284 selected by the consumer 54. For example, if the selected mode of payment was a credit card, then the proxy server 254 may present the consumer 54 with a web page that secures funds by credit card as known in the art. Alternatively, if the selected mode of payment was a prepaid account as described above, then the proxy server 254 may present the consumer 54 with a verification window 144 as shown in FIG. 6, with the funds for the transaction being thereafter debited from the prepaid account.

Upon securing funds for the transaction, the proxy server 254 may then verify the mode of payment accepted by the merchant 56 (step 294). For example, if the merchant 56 has an existing relationship with the proxy management system 252, then funds can be transferred to the merchant (step 295) in accordance with a predetermined agreement or analogous to that described above. Alternatively, if the merchant 56 only accepts credit card payments, then the

proxy server 254 may initiate a credit card transfer as known in the art. Additionally, funds may be transferred with conventional bank transfers. Moreover, the proxy server 254 may be configured to transfer funds to the merchant 56 in the form of a check or a money order, as described in more detail below.

5 Upon receipt of the funds and any other payment information, e.g., shipping address (step 296), the merchant 56 may then transmit a verification signal (step 297) to the proxy server 254. In turn, the proxy server 254 may transmit a payment confirmation web page or e-mail (step 298) which is received by the consumer's computer 80 (step 299).

10 As valid payment has been made, fulfillment of the transaction is carried out, including the merchant 56 providing the goods or services of the transaction (step 301) to the consumer (step 302). The merchant 56 may also provide a service fee to the proxy management system 252 (step 303) for acting a middleman in the transaction, such as an affiliate fee. The consumer 54 may also continue to access merchant web sites (step 304) as desired.

15 In addition to the advantages described above, the proxy management system 252 acts as a payment middleman in handling a transaction between the consumer 54 and the merchant 56. The proxy server 254 may be configured to accept many different types of payment methods, as well as payment methods yet to be developed, without requiring the merchant web site 118 to be constantly updated to accept new and different payment methods. In addition, the billing and payment information of the consumer 54 remains anonymous to the merchant 56 because the
20 proxy server 254 acts as a broker in the transaction, thereby shielding each party from the other party's mode of payment. Therefore, while acting as a broker in the transaction, the proxy server 254 creates a seamless transaction for both the consumer 54 and the merchant 56.

25 In an embodiment of the invention in which the consumer 54 utilizes a prepaid account, shipping address information may be automatically taken from account information previously supplied by the consumer 54. Other fields in the payment window 282 may be left enabled for the consumer 54 to complete.

Single-Use Financial Instrument Transactions

30 As mentioned above, the proxy management system 252 may determine the preferred payment method of a merchant 56 and then transfer funds to the merchant according to that preference. If the preferred payment mode of the merchant 56 is a check, then, according to conventional systems, the consumer 54 would need to write out a check, send the check to the merchant by mail, and then wait for the check to clear before the goods or services are delivered.

If the preferred payment mode of the merchant 56 is a money order, then, according to conventional systems, the consumer 54 would need to purchase a money order from a financial institution, pay a service charge for doing so, and send the money order to the merchant by mail. While checks and money orders are often preferred by many merchants because of the absence of finance charges at their end, clearly both of these conventional approaches have disadvantages to the consumer. For the purposes of this description, check, money orders, and one-time user credit card numbers will be referred to generically as "single-use financial instruments." According to the present invention, the disadvantages to the consumer associated with such instruments, particularly checks and money orders, are substantially eliminated.

Referencing FIG. 10, as mentioned above, the proxy server 254 may be configured to determine the merchant payment mode (step 294). If such determination yield check or money order (step 308), then the proxy server 254 may capture a merchant payment form from the merchant web site 118 (step 310). In addition, the proxy server 254 secures funds from the consumer 54 as described above (step 292), which funds do not need to be in the form of a check or money order. The proxy server 254 then causes the management system 252 to generate a check or a money order (step 312), depending upon the merchant's preference, and then to transmit the check or money order to the merchant 56 (step 314). Accordingly, the proxy management system 252 acts as a payment middleman to provide a seamless transaction regardless of the method of payment at either end of the transaction. In other words, both the consumer 54 and the merchant 56 are able to participate in the transaction utilizing their preferred financial instruments.

More generally, in many embodiments, the consumer 54 will access a merchant web site 118 directly, without first accessing a portal web site 256 and then browsing the merchant web site 118 via the proxy server 254 as described above. In such an embodiment without a proxy server, if the acceptable modes of payment for the merchant 56 include only single-use financial instruments, then the consumer 54 may be burdened to initiate and complete a transaction not according to his or her favored mode of payment. However, according to the present invention, a merchant web site 118 indicates that a single-use financial instrument (e.g., a check or a money order) is the accepted mode of payment, then the consumer 54 may initiate an application on the computer 80 to generate and transfer to the merchant a single-use financial instrument.

For example, if the merchant 56 only accepts checks or money orders, the consumer 54 may initiate an application from the computer to cause the management system 52 or 252 to

capture payment information from the merchant web page 118 and then to generate a single-use financial instrument for the transaction. Once generated, the instrument is transferred to the merchant as though being transferred by the customer 54. Accordingly, as described above, the transaction is seamless to the merchant 54 and allows both parties to partake in transactions on the Internet according to their preferred mode of payment.

As mentioned, the customer 54 does not need to access the proxy server 254 to carry out a transaction with a single-use financial instrument. However, if preferred, the customer 54 may access the proxy server 254 and complete the transaction with the consumer's preferred mode of payment, such as using a credit card or a prepaid account as discussed above. The proxy server 254 may then generate a check or a money order for the transaction and transmit the check or money order to the merchant. Accordingly, the consumer pays funds as desired, and the merchant receives funds as desired. The merchant web page 118 may include a link to the proxy server 254 which, when activated, enables the consumer to complete the transaction utilizing a mode of payment different than that accepted by the merchant.

Surrogate Credit-Card Transactions

According to the present invention, a single-use credit-card number may be generated from a prepaid account for payment of a transaction on the Internet between a consumer and a merchant. For the purposes of this description, the single-use credit-card number will be called a *surrogate number* and, according to a preferred embodiment, may have a fixed amount and a fixed expiration date. The surrogate number may be generated from a credit card of the management system. The amount that is assigned or allocated to the surrogate number may be deducted from the consumer's prepaid account.

Payment with surrogate numbers has multiple applications. For example, the proxy management system 252 shown in FIG. 7 may generate a single-use surrogate number to be used by a consumer 54 for completing a transaction over the Internet 81 with a merchant 56. With reference to FIG. 11, when a consumer 54 initiates a transaction through the proxy management system 252, the proxy server 254 captures and receives the merchant payment information (see steps 277 and 278 of FIG. 8), and then generates a surrogate number (step 320) based on the payment information. The surrogate number may be generated in an amount equal to the purchase price provided by the merchant in the payment information. Alternatively, the surrogate number may include an additional service fee charged to the consumer. In addition, a surrogate number may be generated with a fixed expiration date, for example, within a

predetermined amount of time (such as 24 hours) of generating the surrogate number.

Payment information is then provided to the consumer 54 (step 322), who is prompted to authorize the transaction. When authorized (step 324), the proxy management system secures funds (step 326) from the consumer 54, for example, by debiting a prepaid active account as discussed above. The proxy server 254 then transmits the surrogate number to the merchant server 258 (step 328) which, upon receipt (step 330), may proceed in accordance with the methodology following step 297 of FIG. 8. The generation and the use of surrogate numbers give the proxy management system 252 the security of a conventional credit-card transaction while being valid only for a single transaction with a fixed amount and a short-term expiration date.

The consumer 54 utilizing the management system 250 may request a surrogate number to be generated in a particular amount. The prepaid account associated with the requesting consumer 54 may then be debited for the amount. The consumer 54 now has a valid credit-card number that he or she can use for a single online transaction with a merchant 56. This feature of the invention gives a consumer 54 using the management system 250 the ability to make transactions at merchant web sites accepting credit cards, without the consumer 54 needing to use his or her own personal credit card. In addition, credit-card transactions can be made at web sites not necessarily directly supported by the aforementioned management system, or even if the consumer 54 does not have his or her own personal credit card. The consumer 54 uses the funds in the prepaid account.

The prepaid management system 52 as shown in FIG. 4 may also generate a surrogate number to be used as a refund or a cash-out method for the consumer 54 and his or her prepaid account. For example, the consumer 54 can request a refund for the balance remaining in a prepaid account (i.e., a cash out), rather than requesting the management system 52 to generate and send a check for the balance of funds in the account. The generation of a surrogate number is immediate and without delay. The consumer 54 may then use the surrogate number for any transaction that accepts conventional credit cards.

In addition to an online request as discussed above, the request for a surrogate number may be made remotely through, for example, a wireless application protocol (WAP) interface of the management system 52. By utilizing a WAP interface, a surrogate number can be generated and used at a remote retail location, rather than at a dedicated merchant website. For example, with reference to FIG. 12, a consumer 54 may use a wireless device such as a cellular telephone

to request a surrogate number (step 340) for the total of a dinner tab at a restaurant. Upon receiving the request, the management system 52 may generate the surrogate number (step 342), debit the consumer's active prepaid account (step 344), and transmit the surrogate number to the consumer (step 346). The consumer 54 receives the surrogate number wirelessly (step 348) and provides the number to the merchant (step 350) to complete the transaction. The merchant can then use the surrogate number analogously to a conventional credit-card transaction to complete the transaction (step 352). Accordingly, a consumer 54 is able to complete transactions with a single-use credit-card number, with the funds being deducted from a prepaid account.

Transactions with Anonymous Shipping Addresses

When making transactions over the Internet 81, a consumer 54 may desire to remain anonymous to the e-merchant 56. Anonymity is difficult with regard to the shipping address of the consumer 54. Although a post office address (i.e., a P.O. Box) provides a certain level of anonymity, the name of the post office box holder is public information and may be accessed. In addition, many e-merchants do not accept shipping addresses consisting of post office boxes.

According to the present invention, the anonymity of a consumer 54 making a transaction on the network 58 with a merchant 56 may be maintained. With reference to FIG. 13, when initiating a purchase (step 354), if anonymity is desired (step 356), a consumer 54 may initiate a secure subsession (step 358) with the management system 52. When the subsession is initiated, the management system 52 generates an encoded address (step 360).

The encoded address may be a unique address code stored in a database in the management system 52, for example, in the active accounts database 138 (see FIG. 4), and is associated with the actual shipping address of the consumer 54. The encoded address may be based on consumer input and/or secure point in time information. Preferably, as shown in FIG. 14, an encoded address 361 may include actual information 362 and encoded information 363. The actual information 362 may be the ZIP code of the actual shipping address of the consumer 54 so that the merchant 56 may calculate actual shipping charges. The encoded information 363 may be any type of information that is indecipherable to the merchant, for example, encrypt alphanumeric text. The management system 52 may generate an encoded address associated with a consumer 54 with an actual shipping address at the time the consumer 54 established a prepaid account.

Once generated by the management system 52, the encoded address is provided to the e-merchant 56 (step 364). The encoded address may be provided to the e-merchant 56 either

directly by the management system 52. Alternatively, the management system 52 may provide the encoded address to the consumer 54 who, in turn, may provide the encoded address to the e-merchant 56.

When initiating a purchase (step 354), if anonymity is not desired (step 356), the
5 consumer 54 may provide his or her actual uncoded shipping address to the e-merchant 56 (step 365). In either case, the e-merchant 56 receives the address provided (step 366), be it either encoded or uncoded. The e-merchant 56 may then prepare the goods for shipping (after payment is secured as described above) and deliver the packaged goods to a shipper with the address received from either the consumer 54 or the management system 52 (step 368). The shipper may
10 be either a governmental postal service (e.g., the U.S. Postal Service) or a private carrier (e.g., United Parcel Service, FedEx, etc.)

When received, the shipper determines whether or not the address on the packaged goods is encoded (step 370). This may be done visually or with, for example, an optical scanner. If the address is uncoded, then the goods may be shipped to the consumer 54 (step 372) as usual. If the
15 address is encoded, then the shipper may look up the actual shipping address associated with the encoded address (step 374). The shipper may carry this out by querying the management system 52 which, in turn, may look up or retrieve the actual shipping address from a database and then transmit the same to the shipper. Alternatively, the management system 52 may provide the shipper with the encoded address and the actual shipping address after the encoded address is
20 generated (at step 360). The shipper may store the encoded address and associated actual shipping address in a database and maintain the database of a plurality of encoded addresses and associated actual shipping addresses. In either case, once the actual shipping address is obtained, the goods may be shipped (step 372).

Those skilled in the art will understand that the present invention is not limited to the
25 embodiments specifically illustrated in the drawings and described above. Rather, those skilled in the art will realize that the specific elements of the present invention may be modified and are capable of numerous alternatives without departing from the scope and spirit of the present invention. Accordingly, the scope of the present invention is determined by the terms of the appended claims and their legal equivalents and not by the specific exemplary embodiments shown
30 and described herein.

CLAIMS

What is claimed is:

- 1 1. A method for managing a transaction on the Internet between a consumer and a
2 merchant, the consumer having an actual shipping address, the method comprising:
 - 3 a) receiving a query from the consumer to an anonymous transaction;
 - 4 b) generating an encoded address for the transaction associated with the actual shipping
5 address of the consumer;
 - 6 c) providing to the merchant the encoded address; and
 - 7 d) transmitting to a shipper the actual shipping address.
- 1 2. The method as claimed in claim 1 wherein step (d) comprises:
2 receiving a query from the shipper including the encoded address;
3 retrieving the actual shipping address associated with the encoded address; and
4 transmitting the retrieved actual shipping address to the shipper.
- 1 3. The method as claimed in claim 1 wherein step (d) comprises:
2 transmitting to the shipper the encoded address and the actual shipping address.
- 1 4. The method as claimed in claim 1 further comprising:
2 repeating steps (a) through (d).
- 1 5. The method as claimed in claim 1 further comprising:
2 maintaining a database including a plurality of encoded addresses.
- 1 6. The method as claimed in claim 5 wherein step (b) comprises:
2 establishing a prepaid account with the consumer;
- 1 7. A method for carrying out a transaction on the Internet by a consumer with a
2 merchant with anonymity, the merchant having a merchant web site, the consumer having an
3 actual shipping address, the method comprising:
 - 4 a) initiating a purchase on the merchant web site with the merchant;
 - 5 b) causing a encoded address associated with the actual shipping address to be
6 generated;

- 7 c) causing the encoded address to be provided to the merchant; and
8 d) causing the actual shipping address to be provided to a shipper.

1 **8.** A method for shipping goods purchased by a consumer from a merchant over the
2 Internet, the consumer having an actual shipping address, the method comprising:

- 3 a) receiving an encoded address associated with the actual shipping address;
4 b) retrieving the actual shipping address associated with the encoded address; and
5 c) shipping the goods to the actual shipping address.

1 **9.** The method as claimed in claim 8 further comprising:
2 storing the received encoded address into a database.

1 **10.** A method for carrying out a transaction on the Internet by a consumer with a
2 consumer with anonymity, the consumer having an actual shipping address, the method
3 comprising:

- 4 a) receiving an encoded address associated with the actual shipping address; and
5 b) delivering packaged goods associated with the transaction with the encoded
6 address to a shipper.

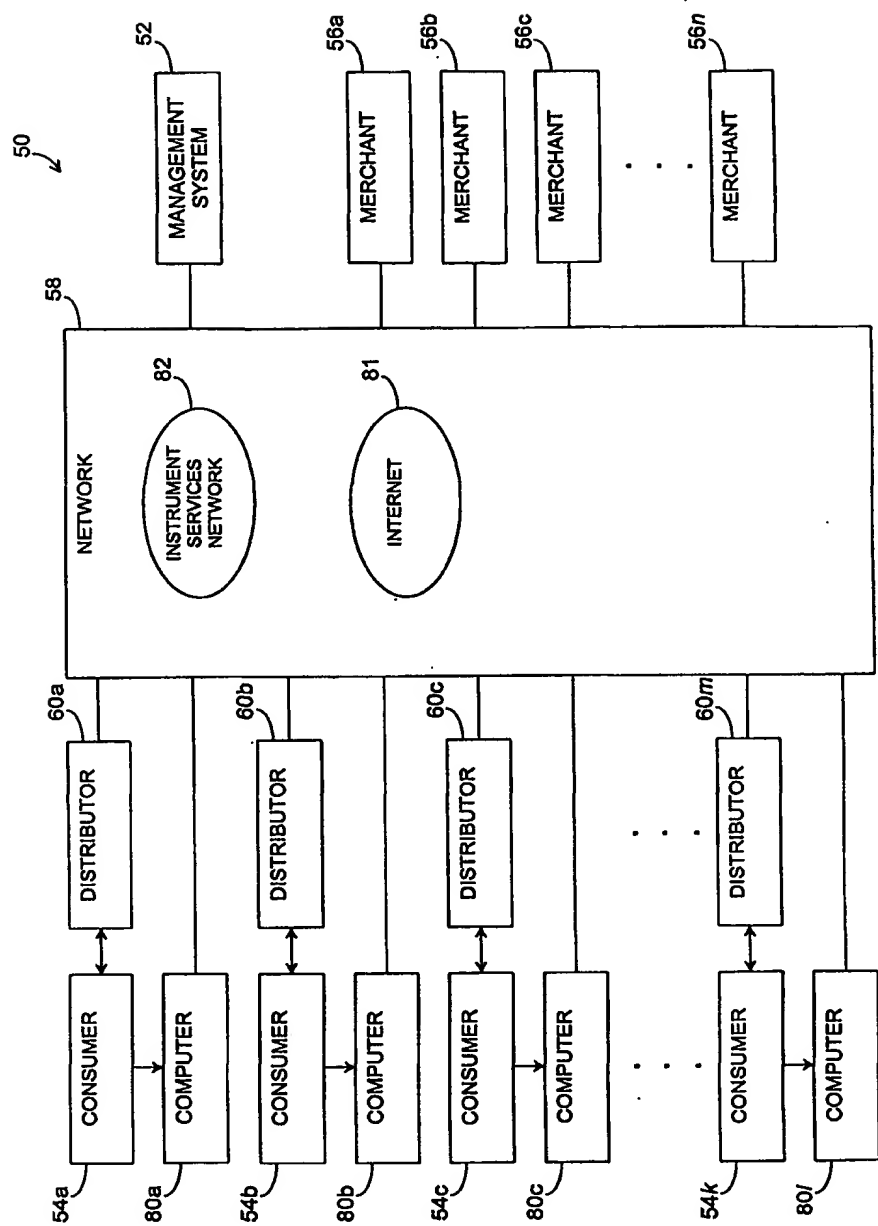


FIG. 1

Internet Activation Browser Window 1

Enter Security Code:

SUBMIT

FIG. 5A

Internet Activation Browser Window 2

Enter User ID:

Enter Password:

Challenge Phrase:

Challenge Response:

SUBMIT

FIG. 5B

\$100.00

Security Code: ABC123456789XYZ

Barcode

FIG. 2

E-Merchant Verification Browser Window

Enter User ID:

Enter Password:

SUBMIT

FIG. 6

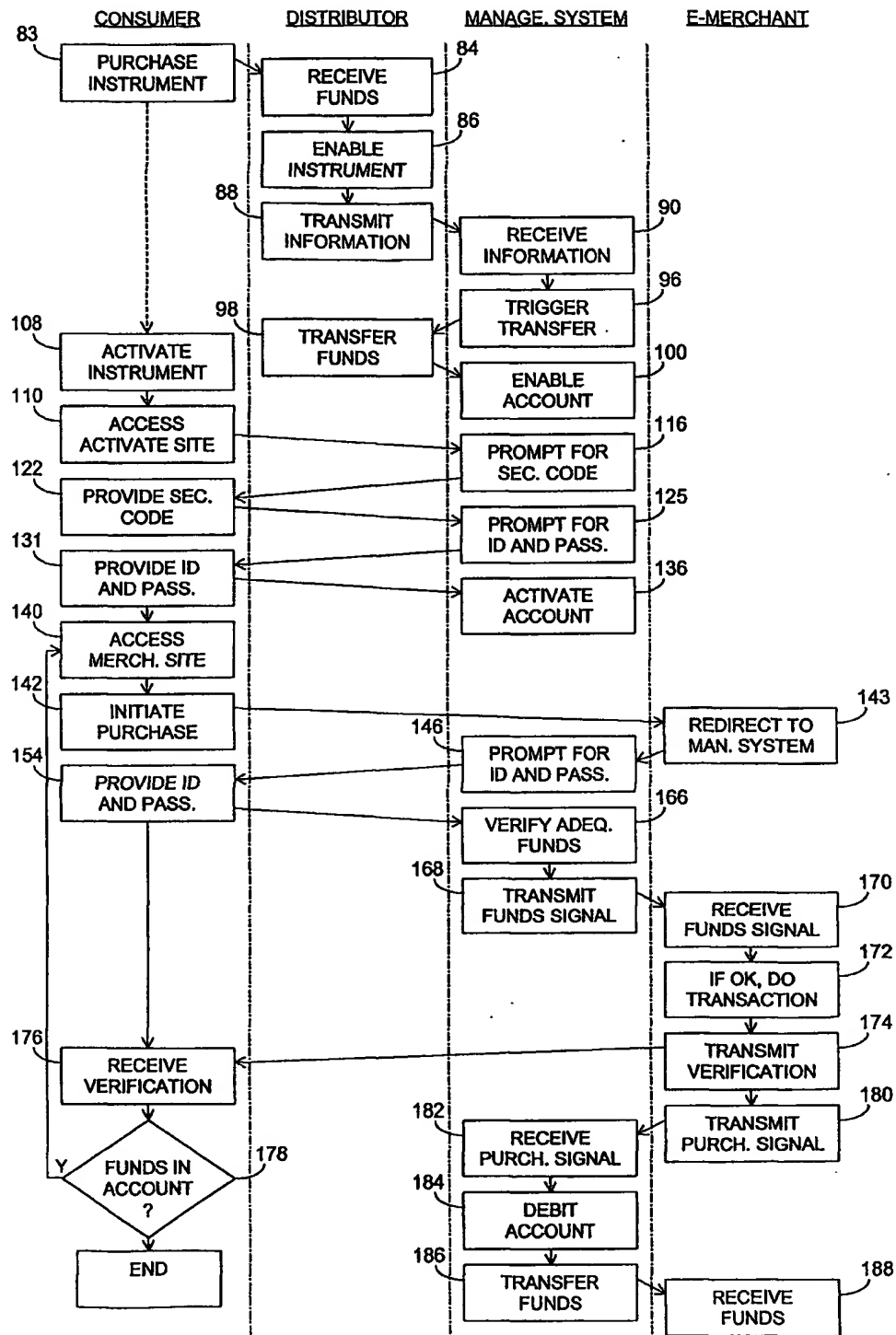
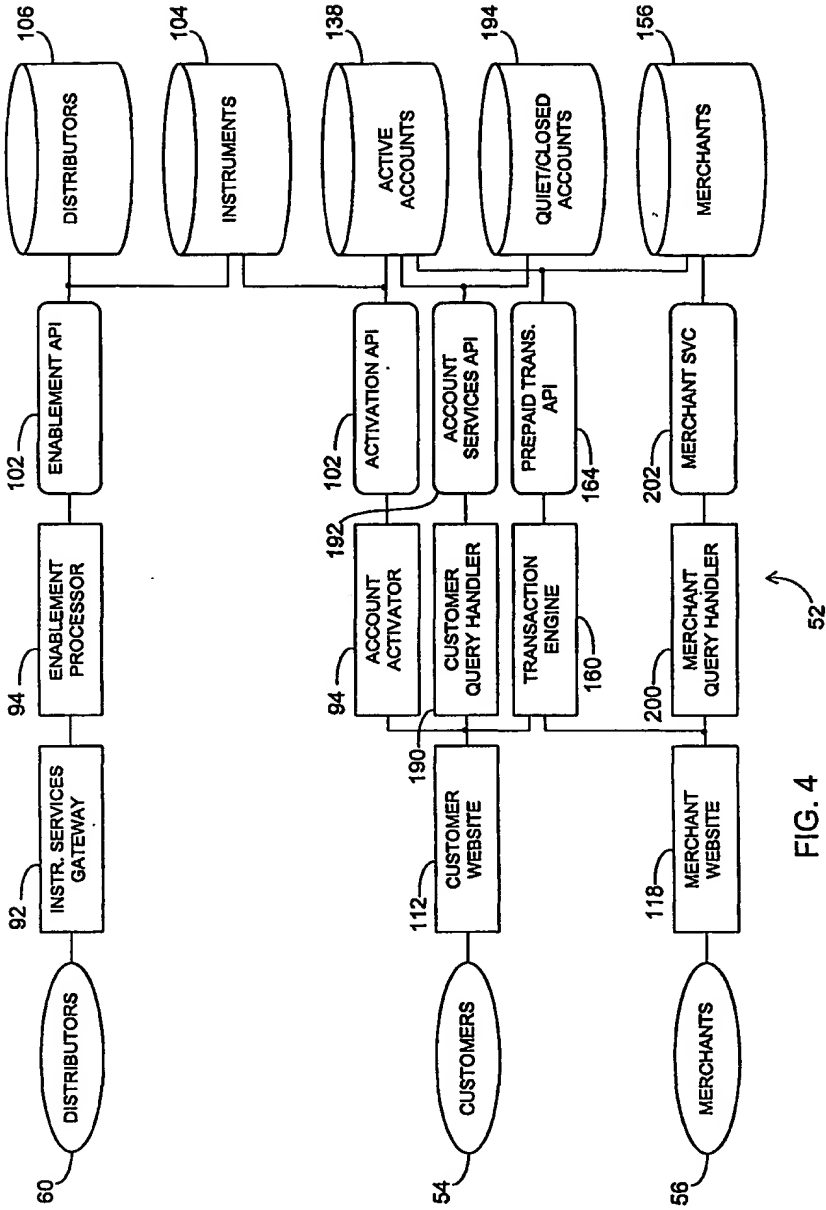


FIG. 3



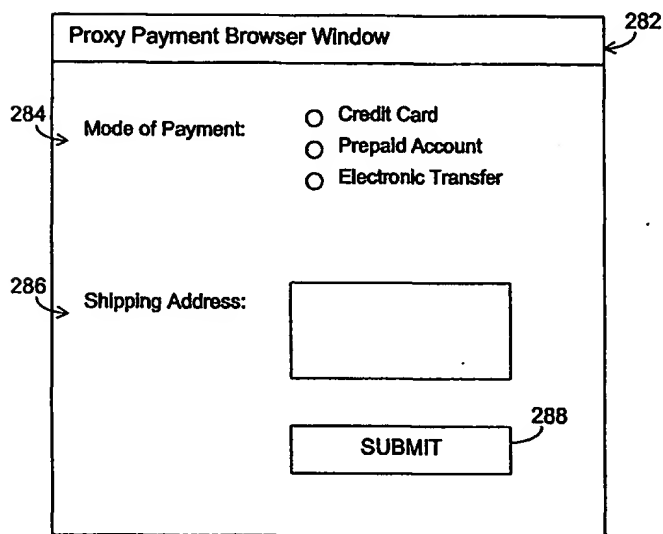
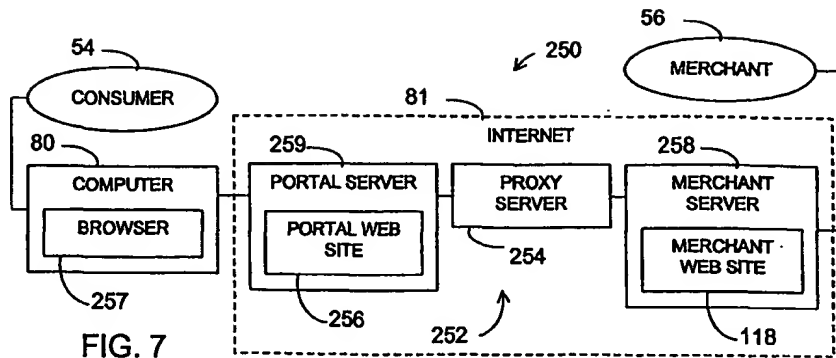


FIG. 9

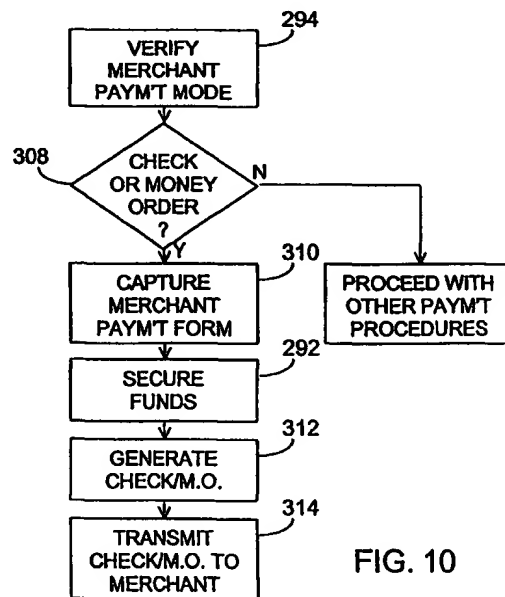


FIG. 10

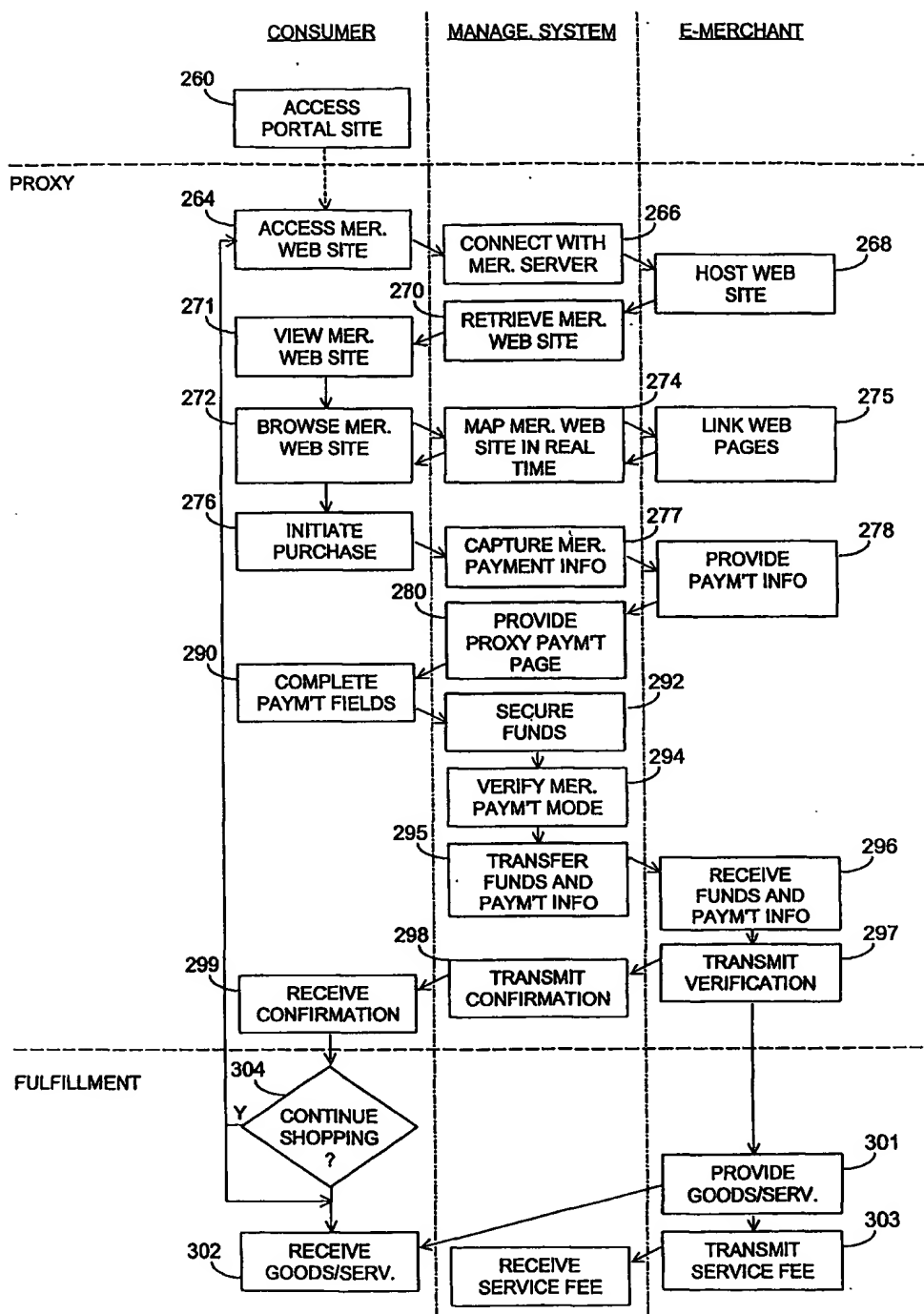


FIG. 8

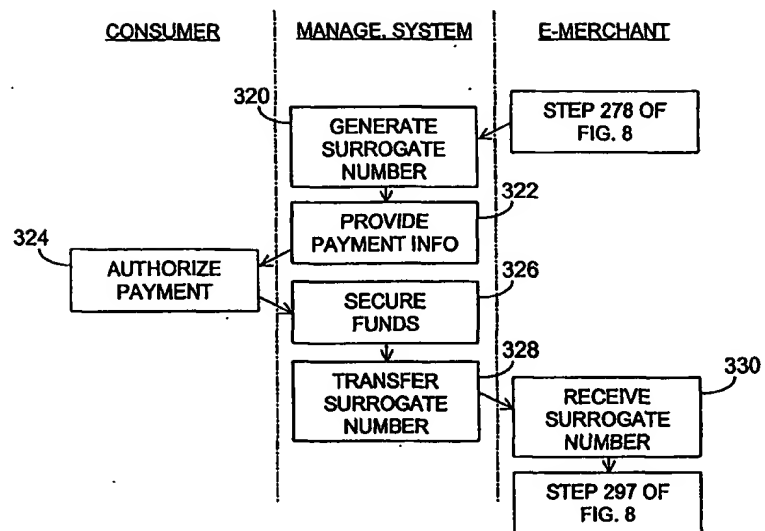


FIG. 11

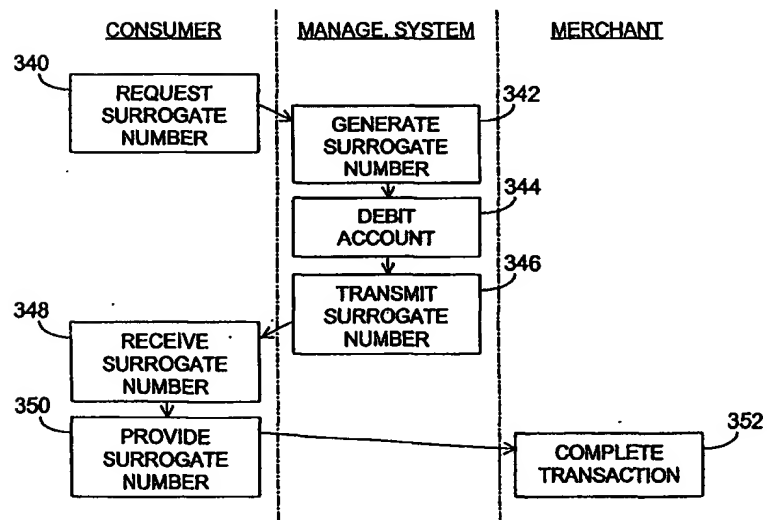


FIG. 12

